MJSAT

Malaysian Journal of Science and Advanced Technology

journal homepage: https://mjsat.com.my/

Simulating the Effectiveness of an IoT Parcel Alert System for Enhancing Delivery Efficiency and Safety During Covid-19

Ahmad Anwar Zainuddin*[1], Hafizah Mansor[1], Nurul Iffah Badrulhisham[1], Nurul Nabilah Zulkifli[1], Aisyah Afiqah Mohd Ridzal[1], and Nasyitah Ghazalli[2]

[1]*Department of Computer Science Kuliyyah Information Communication Technology, IIUM, Malaysia*
[2]*Research and Technology, Thales, United Kingdom*

KEYWORDS

Parcel Delivery Alert System
IoT
Sensors
MARS Simulator

ARTICLE HISTORY

Received 2 February 2023
Received in revised form 26 March 2023
Accepted 30 March 2023
Available online 31 March 2023

ABSTRACT

The Internet of Things (IoT) has revolutionized the way devices communicate and interact with one another. Malaysia has witnessed a substantial increase in online purchasing in recent years. The COVID-19 pandemic and the Malaysian government's mobility control order (MCO) have contributed to the rise in online sales. This circumstance has resulted in a substantial increase in the number of packages that Malaysian delivery firms must manage, producing issues for both homeowners and delivery services. Unattended parcel delivery, parcel loss, and unsuccessful delivery efforts have become widespread. This paper proposes an IoT-based Parcel Delivery Alert System to address the challenges associated with unattended parcel delivery, parcel loss, and failed delivery attempts. The system comprises a parcel safe box that integrates with IoT sensors, such as weight and load sensors, image sensors, and light sensors. The IoT sensors provide real-time information about the delivery status and alert the recipient once the delivery has been made. The system's efficiency and effectiveness were evaluated using the MARS simulator, demonstrating a significant improvement in parcel delivery performance. This paper presents the design, development, and simulation of an IoT-based Parcel Delivery Alert System that can enhance the delivery experience while minimizing delivery-related problems. The paper describes the design and development of the parcel safe box and the eventual evolution of the system. One can acquire access to the safe box by scanning the tracking number on the package's delivery label using a QR code.

1. INTRODUCTION

Amidst the COVID-19 pandemic, parcels have become a common target for theft. However, most parcel boxes currently in use are of the traditional, manual type. This can make parcels less secure if left unattended for an extended period. In situations such as condo, office, and apartment buildings, where mailboxes are located centrally, people may not have sufficient time to inspect their mail or packages. Consequently, even if couriers successfully deliver a package, its safety may still be compromised, even when placed inside the mailbox. The reason for this is that even if the mailbox is secured with a lock or a key, thieves can still open it [1]. Missed deliveries, misplaced shipments, and lengthy delivery procedures are common problems that people all around the world, including Malaysia. A secure parcel box can help protect valuable belongings and mitigate such issues. With the increasing number of online shopping and home deliveries, parcel delivery alert systems have become increasingly important. These systems allow customers to track their packages in real-time and receive notifications upon delivery. Developing a parcel delivery alert system would enable customers to better plan their schedules for receiving packages from the secure box. This application aims to reduce issues faced by customers and couriers while providing a reliable, safe, convenient, and energy-efficient intelligent parcel system. Furthermore, the system offers an

*Corresponding author:
E-mail address: Ahmad Anwar Zainuddin <anwarzain@iium.edu.my>.

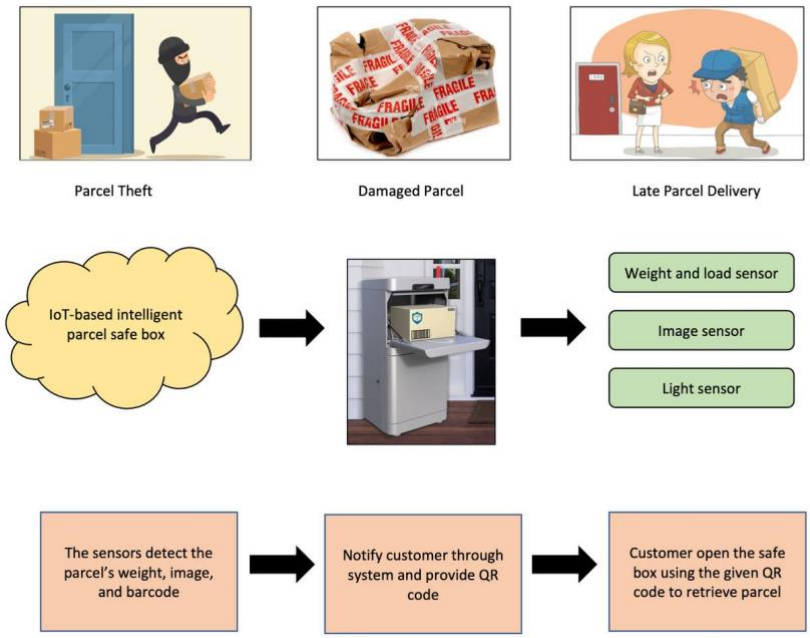

Fig. 1. Graphical Abstract of IoT-Based Intelligent Parcel Safe Box

additional level of security by allowing customers to monitor their deliveries and act if packages are delayed or lost.

This work is to offer an alternative method for individuals to receive their packages by utilizing a secure box as a recipient to accept deliveries from the deliveryman. The proposed system is designed to complete the entire parcel delivery process automatically without requiring any human intervention. Upon placing the parcel in the safe box, the system will notify the recipient through a verification process, which will continue until the parcel is collected. The suggested system comprises a database that maintains all parcel information, parcel verification and authentication, and a security system for the actual parcel box. Figure 1 shows the graphical abstract for this work. The primary objectives of this work are to provide a secure and user-friendly solution to avoid contact with potential risks, prevent theft of parcels, notify users of safe parcel delivery, and ensure successful delivery to the intended recipient. To achieve these objectives, this work proposes an IoT-based intelligent parcel safe box method that incorporates One-Time-Password (OTP) and QR code approaches. The Internet of Things (IoT) is a rapidly growing topic in engineering and technology, garnering attention from both specialized and general media. Its aim is to enable machine-to-machine communication by connecting objects to the internet.

With network computing capabilities built in, the machine can operate independently without the need for human intervention. This technology has been made possible by advances in computer processing power, miniaturization of electronics, and network connectivity, and has been implemented in a variety of networked goods, systems, and sensors, offering new capabilities that were previously impossible [2]. There have been numerous conferences, publications, and news articles discussing and debating the potential impact of the "IoT revolution," covering topics ranging from concerns over security and privacy to technological compatibility and new market opportunities and business models [11]. The IoT devices should be interoperable, self-configuring, have distinct identities, and be able to communicate and exchange data with other devices and systems. They should also be able to dynamically adapt to changing situations and perform actions based on their operational conditions. As a result, smart devices need to be network connected and context aware [3]. Thus, three sensors which are weight and load sensor, image sensor and light sensor to employ in the parcel safe box are used in this work. Overall, this system will provide convenience, peace of mind and added security for customers. This article is presented in the following manner. Section 2 describes the literature overview of this paper; section 3 addresses the methodology that will be applied on this work; section 4 explains the results and discussion of the used of MIPS and MARS simulation and section 5 concludes the paper of how this system works to benefit the customers.

2. LITERATURE REVIEW

2.1 Implementation of Single Cycle Processor

This study focuses on the implementation of a single cycle data path using the Very High-Speed Integrated Circuit Hardware Description Language (VHDL). The single cycle processor is capable of fetching instructions from memory, executing them, and storing the results in a single cycle, as shown in Figure 2. VHDL is an efficient method for digital

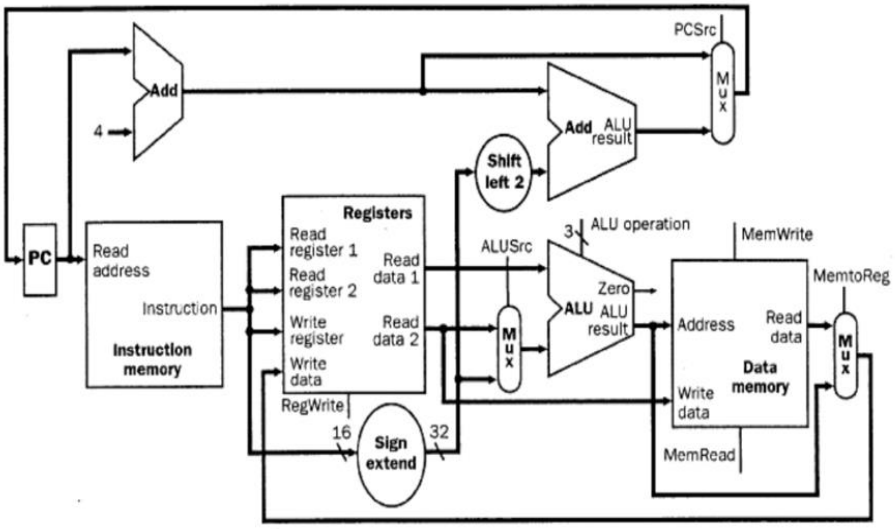

Fig. 2. Datapath of Single Cycle Processor [5].

design entry due to the availability of synthesis tools that aid in the conversion of HDL logic to Field Programmable Gate Array (FPGA) primitives [4].

Single cycle MIPS is a type of Reduced Instruction Set Computer (RISC) processor which has a limited set of instructions that can be executed in a single cycle. The instruction that takes the longest time sets the limit for the cycle time. Therefore, the implementation of the single cycle MIPS processor utilizes a single clock cycle [5]. The RISC processor is equipped with 32-bit memory words, 32-bit general-purpose registers, and fixed-length 32-bit instructions that are classified into three distinct formats, namely J, R, and I. The instructions are executed in parallel as soon as their values become available, resulting in an efficient execution process. To execute an instruction in a single cycle, it requires a sufficiently long propagation delay. However, certain instructions, such as jump instructions that store and write back information into register files, LW, SW, and Load, have a significantly longer propagation delay than others. Arithmetic instructions, such as addition and subtraction, which involve operators such as ADD and SUB, execute quickly but may take up time in each cycle.

2.2 Review on Existing System

Figure 3 illustrates the Ezibox Poslaju, which is a self-service parcel delivery system provided by Poslaju, the national courier company of Malaysia. This system is likely identical to the one presented in the figure, and it is designed to offer customers a convenient and efficient way of sending and receiving packages.

With Ezibox, customers can conveniently drop off their packages at designated locations and monitor the delivery status of their packages online. In summary, Ezibox by Poslaju is a parcel delivery service that prioritizes convenience and efficiency, making the process of sending and receiving packages hassle-free for customers.

Fig 3. Ezibox Poslaju [14]

2.3 Component of The Sensors

2.3.1 Weight Sensor

A weight sensor, also referred to as a weight transducer, is a device that transforms a mechanical force, such as load, weight, tension, compression, or pressure, into another physical variable [12]. In this project, a weight sensor is utilized to detect the weight of a parcel when it is pressed down upon after being placed inside the box. Upon determining the weight, the sensor will notify the owner that the parcel has arrived at the designated box.

2.3.2 Image Sensor

By utilizing this image sensor, an image of the parcel or item that enters the box is captured, and the application is notified to alert the user that their item has been deposited in the designated box. Image sensors can be categorized according to their structure (CCD or CMOS), chroma type (color or monochromatic), and shutter type (global or rolling shutter) [13]. Additionally, image sensors are classified based on their

resolution, frame rate, pixel size, and sensor format. The main objective of image sensors is to convert incoming light (photons) into an electrical signal that can be viewed, analyzed, or stored. As a crucial component of a machine vision camera, image sensors are solid-state devices. Each year, new sensor types are introduced, featuring improvements in sensor size, resolution, speed, and light sensitivity. To focus the incident light (photons) onto the image sensor, a lens or other optics are used. Depending on whether the sensor is CCD or CMOS, the information is transferred to the next stage as a voltage or a digital signal. CMOS sensors utilize an on-chip Analog to Digital Converter to transform photons into electrons, then into a voltage, and finally into a digital value (ADC).

2.3.3 Light Sensor

These light sensors are photoelectric devices that transform both visible and infrared light energy (photons) into an electrical (electrons) signal. A Light Sensors transmit an output signal indicating the light's intensity. Through assessing the radiant energy that exists in a very narrow range of frequencies basically called "light", and which ranges in frequency from "Infra-red" to "Visible" up to "Ultraviolet" light spectrum. The light sensor is a passive device that converts visible or infrared light energy into an electrical signal output.

Light sensors are also known as "Photoelectric Devices" or "Photo Sensors" because they convert light energy (photons) into electricity (electrons). There are two types of photoelectric devices: which both produce electricity when illuminated, such as photovoltaics or photo missives, and those that transform their electrical properties, such as photoresistors or photoconductors.

The framework of bar code reading. Light sensor works in this work by detecting the barcode on the parcel and QR Code. Both barcode and QR Code consists of white and black bars. The scanners retrieve data by shining a light at a barcode or QR Code, capturing the reflected light, and replacing the black and white bars with binary digital signals.

Reflections are strongest in white and weakest in black. A sensor receives reflections in order to generate analogue waveforms. An A/D converter converts the analogue signal to a digital signal (in binary). Data retrieval occurs when a code system is determined from the obtained digital signal (decoding process).

Other than that, CCD method seems suitable for this work. This method employs a CCD (Charge Coupled Device) semiconductor device, which converts light signals into electric signals. A light is built into the CCD method barcode or QR Code scanner. When a scanner shines this light on a barcode or QR Code, the reflection is captured by a CCD and read. A barcode or QR Code is captured only once, allowing for quick reading. There are no moving parts, and the impact resistance is exceptional.

2.4 Technical Information of Sensors

The following tables (Tables 1 -3) are the specifications of the technical information of sensors applied.

Table 1. Technical Information of Weight and Load Sensor

IoT Device	Voltage Range	Input Impedance	Output Impedance	Output Sensitivity
Weight and load sensor	5V to 15 V	055 ± 15 Ω	1000 ± 5 Ω	1.0 ± 0.15 mV/V

Table 2. Technical Information of Image Sensor

IoT Device	Voltage Range	Digital Outputs	Output Signal Amplitude	Spectral Sensitivity Range
Image Sensor	2.5 V to 5V	8 bits to 16 bits	0.6V	400 - 1000 nm

Table 3. Technical Information of Light Sensor

IoT Device	Voltage Range	Operating Current	Output Digital	Output Analog
Light Sensor	13.3V to 5V DC	15mA	0V to 5V	0V to 5V

2.5 Network Protocols

OSI Model is an open access system interconnection reference model, is a very good agreement defined protocol specifications. OSI model has seven layers; each layer can have several sub-layers. According to the comparison of OSI and TCP/IP, and research based on the OSI model implementation models and protocols of the Internet, and the OSI model of data transmission between the layers [6]. In this work, a parcel delivery alert system can use a network such as Wi-Fi to communicate with the delivery company's servers, receive updates and they will notify the customer on the status of a package. For example, in this work, a package that have been placed in the locker being sense by all the sensor involved, then it will be updated in the system. Once it is being updated, it will send the notification of the package's details to the owner of the package or the customer.

In all of this processes, it will use the Wi-Fi which in this case it involves the Physical Layer (Layer 1) and Datalink Layer (Layer 2) of OSI Model. The 802.11 protocol operates in two distinct OSI layers: Layer 1 and Layer 2. The fact that Layer 1 is labelled "Physical" does not imply that it must be physical cabling; radio transmissions are often used here. Layer 1 describes the frequency and modulation forms applied in this case, as well as the pre-amble to lets the transmissions to optimise. Layer 2 is where MAC addresses and BSSIDs are used. Layers 3 and above do not directly apply here, but they are completely reliant on Layers 1 and 2 functioning smoothly.

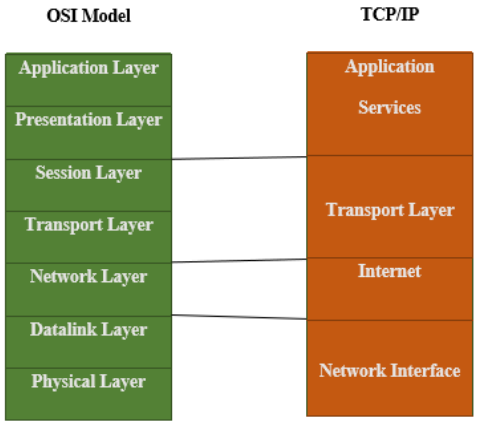

Fig 4. OSI Model

Other than that, on Figure 4 shows the role in the OSI Model or layers are involved 4 services in TCP/IP which are application services, transport, internet, and network interface. In application services it is involve both application layer and presentation layer in OSI Model. Transport services involve session and transport layer, internet involve network layer and network interface involve datalink and physical layer. Whenever a user interacts with a system, the application layer generates an HTTP packet that will eventually be transmitted. This packet initiates the TCP process in the Transport Layer protocol, creating an adjacent layer interaction on the same device. In this interaction, the higher layer (HTTP) requests the lower layer protocol (TCP) to perform the service, and the lower layer carries out the service for the layer above it. This communication continues until the data reaches the final layer. TCP's main purpose is to establish a session with the TCP process on the server, creating a conduit for data transmission between the end user and the server. TCP appends its own information to the top of the HTTP packet to keep the session open. When the packet is in the pending state, TCP hands it over to an IP process, which assigns IP addresses and routes packets to the correct address. The network access layer is responsible for defining protocols and hardware for data transmission across a physical network. The end user encapsulates an IP packet within an Ethernet header and trailer, creating an Ethernet frame with a MAC address for local transmission. The end user uses electricity to transmit the Ethernet frame's bits through the Ethernet cabling. The server receives the electrical signal and de-encapsulates the IP packet from the Ethernet frame by removing the header and trailer. The server reads the TCP data before passing it to the HTTP process, which interprets the get request. The server then sends the requested page to the end user using the same method.

3. METHODOLOGY

3.1 Flowchart

Figure 5 illustrates the flowchart of the Parcel Delivery Alert System, while Figure 6 displays a detailed flowchart with three distinct parts - Part A, Part B, and Part C - representing different stages. In Figure 7, a use case for the Parcel Delivery Alert System is depicted, involving three actors: the Delivery Guy, Recipient, and System.

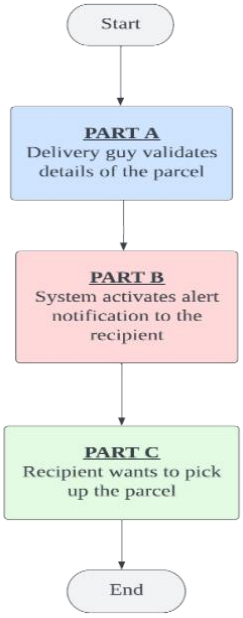

Fig 5. Flowchart Implementation MIPS Assembly Approach

4. RESULT AND DISCUSSION

4.1 MIPS and MARS Simulation

In this work, the MIPS Assembler and Runtime Simulator is used to run the simulation. The codes will illustrate two screens which are delivery guy's screen and recipient's screen. Delivery guys need to ensure recipients' image and weight parcel are being detected before leaving the screen. Weight and load sensor will detect the parcel's weight while the image sensor captures the image of the parcel. If both sensors are successfully detected, the system continues to start barcode detection. This involves the implementation of a light sensor by capturing the barcode to obtain all the information about parcel including parcel_ID variable that will generate the unique Quick Response (QR) code. Figure 8 shows the results of the detection of the weight, image, and barcode when the process was successfully. It also shows the information of recipient and QR code.

Information about parcel details will be sent to the recipient and the recipient needs to verify the parcel details. When the recipient wants to pick up the parcel, the recipient will show QR code and light sensors detect light and convert light energy to an electrical signal output. After detection of QR code is successful, the recipient will receive a One-Time Password (OTP) to verify the authorized recipient only. Recipient needs to enter that password correctly to collect their parcel from the locker. Below is the output of the codes that were implemented using MIPS Assembler and Runtime Simulator.

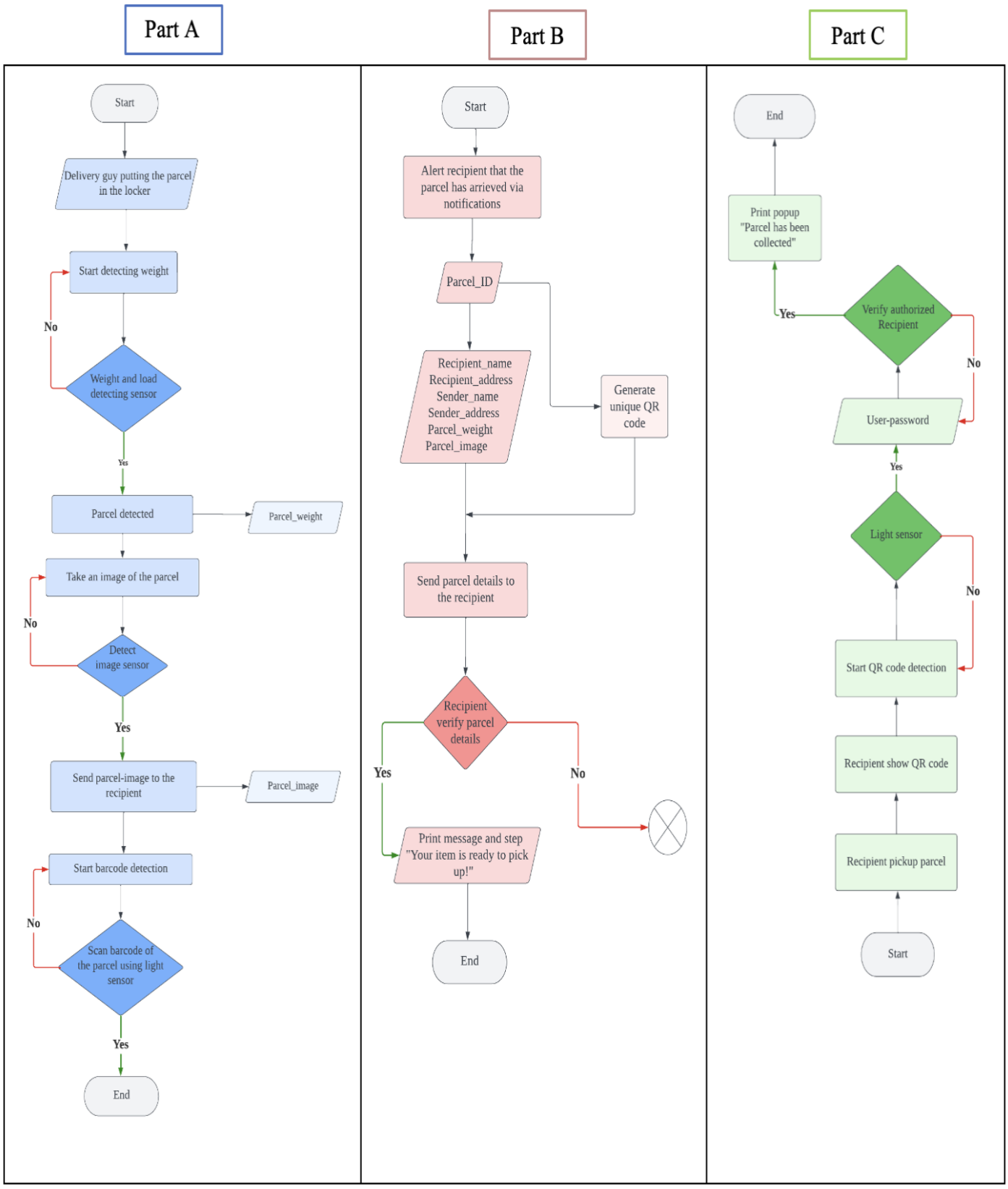

Fig 6. Three Parts of The Implementation MIPS Assembly Approach

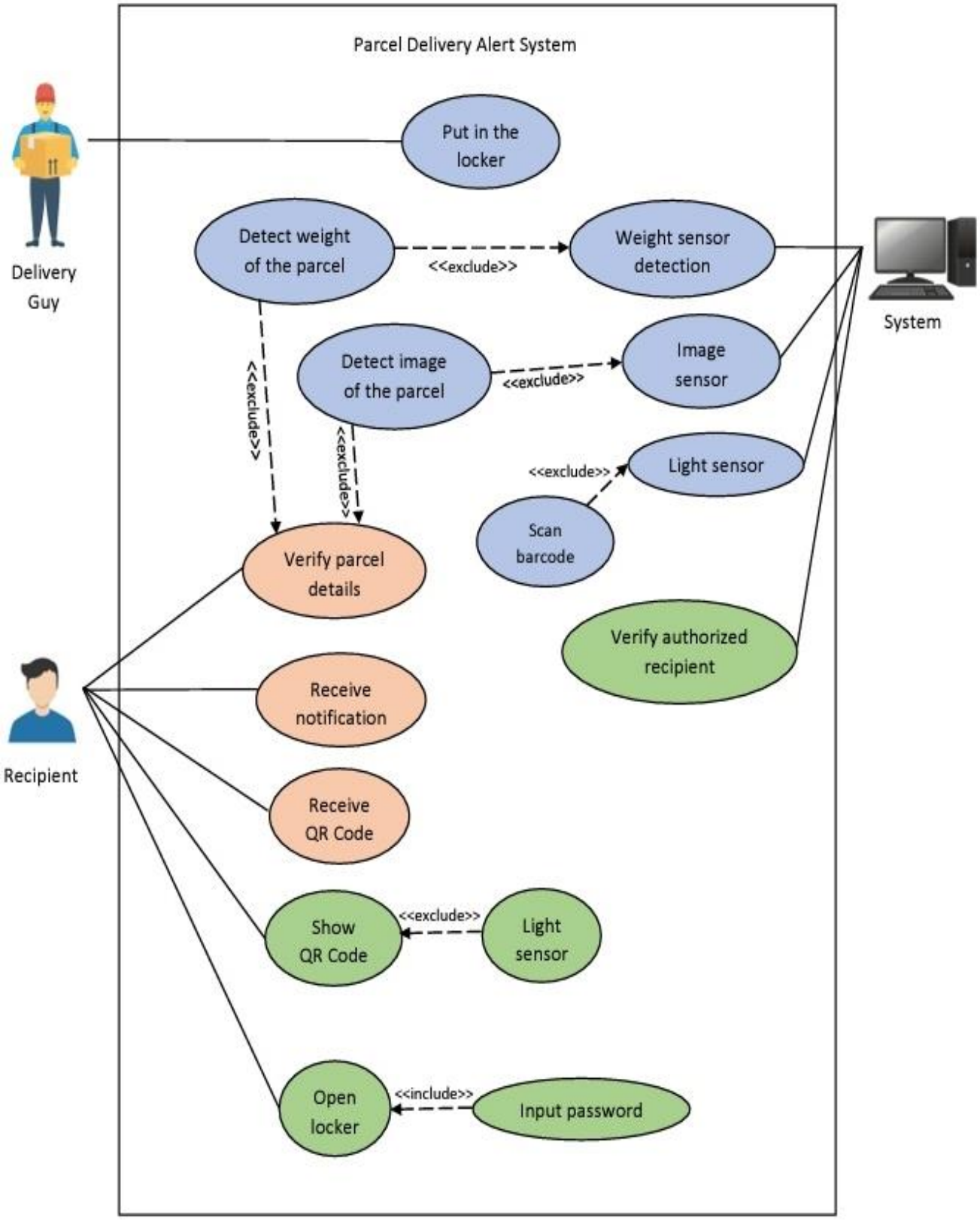

Fig 7. Use Case Diagram of Parcel Delivery Alert System

4.2 IoT Sensors and Implementation

4.2.1 Implementation of Intrusion Detection System (IDS)

The Internet brought about a revolution by connecting the entire world to share information on a single platform. Data is the most valuable asset, every organisation invests heavily in various security solutions such as firewalls, antiviruses, and so on to protect its data and resources from unauthorised access and cyber-attacks such as phishing, hacking, eavesdropping, and so on. Despite the majority of these security mechanisms, hackers can still exploit vulnerabilities in web applications to steal user credentials [7]. Intrusion Detection System (IDS) being defined by a system that monitors network traffic for suspicious activity and alerts when such activity is discovered. IDS is classified by two categories which are Intrusion Detection System on a Network (NIDS) and Intrusion Detection System Based on the Host (HIDS). An Intrusion Detection System on a Network (NIDS) monitors and analyses network traffic to detect network threats. It equates the previous snapshot of the file set to the entire system's file set. The system then notifies the administrator if there is a change in the system's normal behaviour.

```
*******This is delivery guy's screen**********
REMINDER : Please Make Sure Customer's Parcel WEIGHT and IMAGE are being detected
Please enter parcel weight(in kg)= 2

The sensor is detecting the weight of parcel.....
Parcel Weight : 2kg detected!
The sensor is detecting the image of parcel.....
Is detection success(1) or fail(0)?0
Image not detected
Is detection success(1) or fail(0)?1
Parcel's image has been sent to recipient!
THANK YOU!!

*******This is recipient's screen**********
This is your parcel's image!



The sensor is detecting the barcode of parcel.....
Is detection success(1) or fail(0)?0

Barcode detection is unsuccessful!
Is detection success(1) or fail(0)?1

Barcode detection is successful!
Your parcel has arrived!

Here is your information:
NAME: SUZY.
PHONE NUMBER: 012-2239152.
EMAIL: suzy@gmail.com


  Here is the QR code given to open the box !
  Here is your parcel details.
  TYPE OF PARCEL: ITEM
  NAME OF SENDER: WATSON
  SHIP FROM: SHAH ALAM
  SHIP BY DATE: 20/1/23
  TRACKING NUMBER: 6201200905172 93
  ORDER ID: 221201H87XB6AJ

  Please verify your parcel. (if yes enter Y, if no enter N)) y

  The sensor is detecting the barcode of parcel.....
  Your OTP number is : 58942
  Don't share your OTP to others
  Please enter your one time password: 58942

  OTP accepted, proceeding...
  Locker is opening...
  Parcel has been collected!
  -- program is finished running --
```

Fig. 8. Output of Codes Using MIPS Assembler and Runtime Simulator.

Figure 9 shows the implementation of Intrusion Detection System (IDS) in this work to protect system from attacks like Distributed-Denial-of-Service Attack (DDoS), Denial-of-Service Attack (DoS), Hello Flood Attack and Sybil Attack that frequently being aim towards IoT systems. This Intrusion Detection System (IDS) are also being proposed to detect malicious activity in the network and mitigate cyber-attacks [10]. Figure 10 shows the implementation IDS on the parcel delivery alert system. This figure indicates the use of entity authentication and One time Password (OTP) in this work is to implement multifactor authentication to confirm the parcel belongs to the owner.

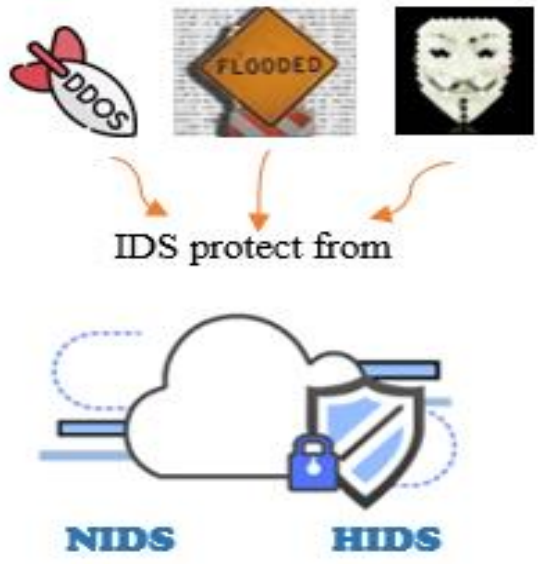

Fig 9. Implementation of Intrusion Detection System (IDS)

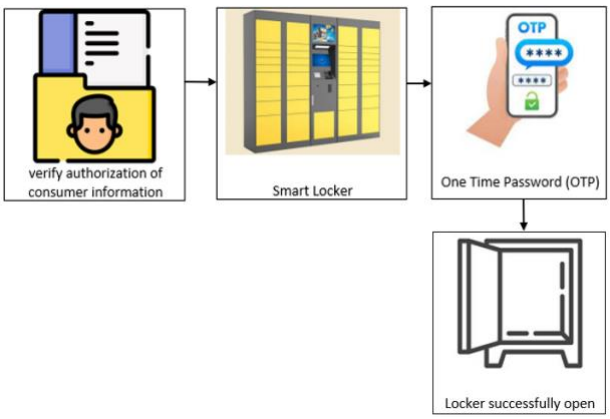

Fig. 10. IDS on the Parcel Delivery Alert System

The authentication verification method is used to secure the package by sending a notification to the package owner to verify the owner's identity. When owner of the package has been verified as the owner, then all package information is sent to the owner so that the user's personal information is not disclosed to irresponsible individuals. Other than that, the use of One Time Password (OTP) message in this system is used as the second step (second factor authentication) for security purposes to ensure that the package is picked up by the owner

of the package by sending an OTP message to the user's phone number so that they can open the box.

4.3 Smart Locker Terminals

The smart lockers terminals are parcel-capable locker units located in convenient and public locations in residential neighbourhoods, storing packages for all customers in a specific area for the time that been set within a few days and serving as automated consolidation delivery points [8]. Customers can pick up their belongings at their convenience by logging into an intelligent terminal linked to the delivery company's system via the Internet of Things (IoT) and entering a code sent in the telephone number. Though this solution requires the customer to leave their home to retrieve the package, if the units are strategically placed throughout the city, it will only take a few minutes to access it, especially if the customer has the option of selecting the most convenient location available, with the option of selecting a unit somewhere on the customer's commuting path.

Furthermore, by eliminating the final step of home delivery, transportation companies will be able to consolidate their parcel deliveries by unit and effectively place the packages in the smart lockers at any time, reducing congestion. Smart Locker Terminals is analogous to Access Points, which are business partners that serve as carrier consolidation delivery points. The distinction is for the customer, who has no human interactions because Smart Locker Terminals are automated units. They are also available at any time, as business hours are no longer a constraint, depending on the terminal's location.

5. CONCLUSION

This work examines an alternative method for consumers to access their packages or parcels through a parcel delivery alert system, aiming to prevent theft incidents and ensure delivery to the rightful recipient. Our proposed solution is an IoT-based intelligent parcel safe box that utilizes a one-time password (OTP) and QR code approach, providing a secure, authentic, and user-friendly method of access. The incorporation of QR codes and OTPs could provide an additional layer of security to the safe box. The Internet of Things (IoT) has garnered significant attention in engineering and technology industries for its potential to enable machine-to-machine communication by connecting everyday objects to the internet. Integrating a parcel delivery alert system with a safe box could greatly enhance the convenience and efficiency of parcel delivery, offering real-time updates and notifications to customers regarding their delivery status. Utilizing a safe box for package storage could also enhance delivery security by securely storing packages until the recipient retrieves them, minimizing the risk of theft or tampering. Overall, this parcel delivery alert system could improve the customer experience and satisfaction with the parcel delivery process.

REFERENCES

[1] M. Mokhsin, M. Z. M. Ludin, A. I. H. Suhaimi, A. S. Zainol, M. H. Mohd Som, and H. A. Halim, "ParcelRestBox: IoT-Based Parcel Receiving Box System Design for Smart City in Malaysia," in 2021 IEEE International Conference on Computing (ICOCO), Kuala Lumpur, Malaysia, Nov. 2021, pp. 180–185. doi: 10.1109/ICOCO53166.2021.9673588.

[2] S. Mahendra, M. Sathiyanarayanan, and R. B. Vasu, "Smart Security System for Businesses using Internet of Things (IoT)," in 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT), Bangalore, India, Aug. 2018, pp. 424–429. doi: 10.1109/ICGCIoT.2018.8753101.

[3] M. Silverio-Fernández, S. Renukappa, and S. Suresh, "What is a smart device? - a conceptualisation within the paradigm of the internet of things," Vis. Eng., vol. 6, no. 1, p. 3, Dec. 2018, doi: 10.1186/s40327-018-0063-8.

[4] "Difference Between Single-Cycle and Multi Cycle Processor", doi: 10.34218/IJEET.11.10.2020.034.

[5] T.-T. Hoang et al., "Low-power high-performance 32-bit RISC-V microcontroller on 65-nm silicon-on-thin-BOX (SOTB)," IEICE Electron. Express, vol. 17, no. 20, pp. 20200282–20200282, Oct. 2020, doi: 10.1587/elex.17.20200282.

[6] Y. Li, D. Li, W. Cui, and R. Zhang, "Research based on OSI model," in 2011 IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China, May 2011, pp. 554–557. doi: 10.1109/ICCSN.2011.6014631.

[7] S. Zaman, H. Tauqeer, W. Ahmad, S. M. A. Shah, and M. Ilyas, "Implementation of Intrusion Detection System in the Internet of Things: A Survey," in 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, Nov. 2020, pp. 1–6. doi: 10.1109/INMIC50486.2020.9318047.

[8] S. Wei, "Research and Application of Smart Lock Safety Management and Control System," J. Phys. Conf. Ser., vol. 1601, no. 5, p. 052038, Aug. 2020, doi: 10.1088/1742-6596/1601/5/052038.

[9] Y. Vakulenko, D. Hellström, and K. Hjort, "What's in the parcel locker? Exploring customer value in e-commerce last mile delivery," J. Bus. Res., vol. 88, pp. 421–427, Jul. 2018, doi: 10.1016/j.jbusres.2017.11.033.

[10] M. Husnain et al., "Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System," Sensors, vol. 22, no. 2, p. 567, Jan. 2022, doi: 10.3390/s22020567.

[11] Walczak, R., Koszewski, K., Olszewski, R., Ejsmont, K., & Kálmán, A. (2023). Acceptance of IoT Edge-Computing-Based Sensors in Smart Cities for Universal Design Purposes. Energies, 16(3), 1024.

[12] Kumar, V. S., & Krishnamoorthi, C. (2021). Development of electrical transduction based wearable tactile sensors for human vital signs monitor: Fundamentals, methodologies and applications. Sensors and Actuators A: Physical, 321, 112582.

[13] Parulski, K., & Spaulding, K. (2017). Color image processing for digital cameras. In Digital color imaging handbook (pp. 727-757). CRC Press.

[14] Reterived from " http://hanisyahida.blogspot.com/2017/08/ezibox-upm-kmr.html"